MILBERG LLP
DAVID AZAR (SBN 218319)
dazar@milberg.com
2850 Ocean Park Blvd. Suite 300
Santa Monica, CA 90405
Telephone: (213) 617-1200
Facsimile: (212) 868-1229
Attorneys for Plaintiff and the Proposed Class

[Additional Counsel Listed on Signature Page]

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

BRIAN NEFF, individually and on behalf of all others similarly situated,

Plaintiff,

v.

YAHOO! INC., and AABACO SMALL BUSINESS, LLC.,

Defendants.

Case No.

CLASS ACTION COMPLAINT FOR:

1. **Breach of Contract**
2. **Breach of Implied Contract**
3. **Negligence**
4. **Fraudulent Inducement**
5. **Negligent Inducement**
6. **Violations of the California Unfair Competition Law, Business & Professions Code § 17200, *et seq.***

JURY TRIAL DEMAND

Plaintiff Brian Neff ("Plaintiff" or "Mr. Neff") brings this Class Action Complaint against defendants Yahoo! Inc., and Aabaco Small Business, LLC (respectively "Yahoo" and "Aabaco," and collectively "Defendants"), on behalf of himself and a national class of Yahoo Small Business/Aabaco Small Business customers (the "Class Members" or "Class"), and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION and INTRODUCTION

1. Yahoo, directly and through its wholly owned subsidiaries like Aabaco, offers various online services to consumers and small businesses. This action concerns the business services utilized by small businesses and/or their owners, who paid monthly fees for those services. Popular services include website hosting, which makes it easy for businesses to create and operate a business website, advertising for those businesses, and email services for communications between businesses and their customers and others.

2. Yahoo originally provided these services through a division called Yahoo Small Business. Since November 2015, Yahoo has provided its small business services through its wholly-owned subsidiary Aabaco. After the switch, Yahoo informed Class Members that the change was in name only, greeting them with the following account sign-in notice: "Yahoo Small Business is now Aabaco Small Business. Same Team. Same Passion to grow your business. Different name." Exhibit A attached hereto.

3. When small business customers establish accounts with Defendants, Defendants collect and electronically store their personally identifiable information ("PII"), such as names, email addresses, telephone numbers, dates of birth, passwords, and, in some cases, security questions and answers. This information is a treasure trove for hackers who can use the information to profit by causing damage to Defendants' small business customers, as occurred here.

4. Mr. Neff brings this class action against Defendants for their failure to secure their users' PII and for their failure to provide timely, accurate, and adequate notice to him and

other Class Members that their PII had been stolen on at least two occasions, causing significant damage to them.

5. On September 22, 2016, Yahoo announced that certain user account information was stolen from its systems in late 2014 (the "2014 Data Breach"), more than two years earlier. Subsequently, Yahoo sent individual email notifications to all users it believes were affected by the breach, including many Class Members. Yahoo conceded that the theft included PII, such as users' names, email addresses, telephone numbers, dates of birth, passwords, and, in some cases, security questions and answers. Yahoo claimed that the stolen information did not include payment card data or bank account information, as payment card data and bank account information were allegedly not stored in the system that its investigation had found to be affected. Yahoo did not disclose the 2014 breach until over two years after it occurred.

6. On December 14, 2016, Yahoo disclosed an earlier and even larger data breach. In August 2013, hackers obtained the PII of more than 1 billion Yahoo users (the "2013 Data Breach"). According to Yahoo's December 14, 2016 press release, in the 2013 Data Breach, hackers stole user account information that "may have included names, email addresses, telephone numbers, dates of birth, hashed passwords and, in some cases, encrypted or unencrypted security questions and answers."[1] It is unclear whether the stolen information included passwords in plain text, payment card data, or bank account information. Yahoo did not disclose the 2013 Data Breach until more than three years after it occurred.

7. In addition to the press release, Defendants informed Mr. Neff and many Class Members of the 2013 Data Breach by individual email notice, stating as follows, in relevant part:

> Dear Brian,
>
> We are writing to inform you about a data security issue that may involve your Yahoo account information. We have taken steps to secure your account and are working closely with law enforcement.

[1] Yahoo press release, "Important Security Information for Yahoo Users," Dec. 14, 2016, *available at* https://investor.yahoo.net/ReleaseDetail.cfm?&ReleaseID=1004285 (last visited Feb. 8, 2017).

> What Happened?
>
> Law enforcement provided Yahoo in November 2016 with data files that a third party claimed was Yahoo user data. We analyzed this data with the assistance of outside forensic experts and found that it appears to be Yahoo user data. Based on further analysis of this data by the forensic experts, we believe an unauthorized third party, in August 2013, stole data associated with a broader set of user accounts, including yours.
>
> We have not been able to identify the intrusion associated with this theft. We believe this incident is likely distinct from the incident we disclosed on September 22, 2016.
>
> What Information Was Involved?
>
> The stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers. Not all of these data elements may have been present for your account. The investigation indicates that the stolen information did not include passwords in clear text, payment card data, or bank account information. Payment card data and bank account information are not stored in the system we believe was affected.

Exhibit B attached hereto.

8. Only now, three years after the 2013 Data Breach, are Defendants notifying potentially affected users and requiring users to change their passwords. Defendants have also invalidated unencrypted security questions and answers so that they cannot be used to access an account. Yahoo declined to take these steps after its September 2016 disclosure of the 2014 Data Breach,[2] despite those steps constituting the absolute minimum precautions that Yahoo and its customers should have taken following a data breach to protect the customers from identity theft and other fraud.

9. At this early stage, it is unknown to Mr. Neff whether Yahoo's descriptions of the breadth of the Data Breaches are accurate. However, given that more than three years elapsed before Yahoo disclosed the 2013 Data Breach and more than two years passed before Yahoo disclosed the 2014 Data Breach, Mr. Neff is rightfully skeptical of Yahoo's self-serving

[2] *See* Vindu Goel and Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked,* N.Y. Times, (Dec. 14, 2016), http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=1 (last visited Feb. 8, 2017).

statements. Although, Yahoo claims that it only discovered the 2013 Data Breach in November 2016 while investigating the 2014 Data Breach, that remains to be proven.

10. Defendants violated Mr. Neff's and Class Members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their data systems were protected, failing to take available steps to prevent and stop the 2013 Data Breach and 2014 Data Breach (collectively, the "Data Breaches") from happening, failing to promptly disclose the theft of Mr. Neff's and Class Members' PII via the Data Breaches, and failing to disclose to Mr. Neff and Class Members the material facts that they did not have adequate computer systems and security practices to safeguard Mr. Neff's and Class Members' PII. Mr. Neff is informed and believes that his and Class Members' PII was improperly handled and stored, was unencrypted or inadequately encrypted, and was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Mr. Neff's and Class Members' PII was compromised and stolen. However, as the same or updated information remains stored in Yahoo's computer systems, Mr. Neff and Class Members have an interest in ensuring that their information is safe, and they are entitled to injunctive and other equitable relief to prevent future data breaches, including independent oversight of Yahoo's security systems.

PARTIES

11. Plaintiff, Brian Neff, is an individual citizen of Texas. In September 2009, in connection with his online insurance agency business, he contracted with Yahoo for two services, Yahoo! Web Hosting for www.TheInsuranceSuite.com and Yahoo! Business Email, for which he has paid Yahoo $13.94 every month through the date of this Complaint. Between 2009 and the present, at various times, Mr. Neff has utilized Yahoo's webhosting services in connection with another 54 websites, paying anywhere from $3.94 to $15.94 per month for each website. As set forth in detail above, on December 14, 2016, Plaintiff received a notice from Yahoo informing him that hackers had stolen account information that he had provided to Defendants--information that "may have included names, email addresses, telephone numbers,

dates of birth, hashed passwords (using outdated encryption) and, in some cases, encrypted or unencrypted security questions and answers." Exhibit B.

12. In addition to paying Yahoo thousands of dollars for services that subjected him to a security breach, Mr. Neff was also a victim of actual identity theft following the Data Breaches which, upon information and belief, was caused by one or both of those Data Breaches. In May 2015, he incurred fraudulent charges on his Capital One credit card and his Chase debit card, both of which were on file with Yahoo to pay for services connected with two of his websites, with Yahoo being the only company to which Mr. Neff had provided information about both accounts. In addition to these fraudulent charges, also in May 2015, an unauthorized credit card account in Mr. Neff's name was opened at Credit One Bank, and unauthorized and fraudulent charges were made to that account in May and June of 2015. The probability that separate criminals stole card information from separate sources, stole the information necessary to open a new credit card account from a separate source, and made fraudulent charges on all three cards in the same month is staggeringly remote. Mr. Neff had to spend significant time and incurred expenses mitigating the harm to him from these security breaches and identity theft. As to both the Capital One and Chase cards, Mr. Neff had to make several phone calls to each to notify them of the fraudulent charges and to have the accounts frozen. He had to change passwords for both cards and he then had to wait two to four days to receive new cards from each. As to the credit card opened in his name, Mr. Neff had to call the police department and file a police report, fill out an FTC affidavit, engage in multiple phone calls over several weeks totaling multiple hours to Credit One, and put together a package of materials for Credit One, which took hours, and which was sent to Credit One via Federal Express overnight delivery at a cost of $11.87. Since these incidents, Mr. Neff has been reviewing reports from complimentary credit monitoring offered by all his credit cards which offer that complimentary service, reviewing daily updates from Credit Karma, and has ordered and reviewed free annual reports from all three credit bureaus, as to which activities he has devoted many hours of time. Now that he is aware of the inadequacy of Defendants' online security, Mr. Neff intends to migrate his insurance agency website,

www.TheInsuranceSuite.com, to a more secure provider, but given its high level of content (over 100 pages), the complexity of the website's content, including the built-in lead generation forms and communications capacity, and the high SEO earned over the last eight years, he has learned that such a transfer will cost him in excess of $10,000.

13. Yahoo, a Delaware corporation with its principal place of business in Sunnyvale, California, is a technology company offering sites for digital information discovery, focused on informing, connecting, and entertaining its users through its search, communications, and digital content products. It provides small businesses with services such as website building/hosting, business email, and advertising. Yahoo's revenue is generated principally from display and search advertising and paid service offerings.

14. Aabaco is a wholly-owned and controlled subsidiary of Yahoo with its headquarters and principal place of business at the same address as Yahoo's headquarters in Sunnyvale. Since November 2015, it has been the legal entity through which Yahoo has provided services to small business customers.

15. As relevant to this action, Aabaco has acted as Yahoo's alter-ego. The acts complained of herein are the joint acts and responsibility of both Yahoo and Aabaco. As to any wrongful acts carried out by Aabaco alone, Yahoo is liable under a theory of *respondeat superior* and/or alter ego liability. As to any acts preceding Aabaco's inheritance of Yahoo's Small Business enterprise, Aabaco is liable as successor in interest.

JURISDICTION AND VENUE

16. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed $5,000,000.00, exclusive of interest and costs, and this is a class action in which more than two-thirds of the proposed plaintiff class, on the one hand, and Defendants, on the other, are citizens of different states.

17. This Court has jurisdiction over Defendants because they maintain their corporate headquarters in this District and for the following reasons: Defendants make

decisions regarding overall corporate governance and management, including the security measures to protect their users' PII, in this District; they are authorized to conduct business throughout the United States, including California; and they advertise in a variety of media throughout the United States, including California. Via their business operations throughout the United States, Defendants intentionally avail themselves of the markets within this state to render the exercise of jurisdiction by this Court just and proper.

18. In addition, this Court has personal jurisdiction over Defendants pursuant to the California choice of law and forum clause contained in Defendants' Terms of Service agreement entered into between them and all Class Members:

> The Agreement and the relationship between You and the Company shall be governed by the laws of the State of California without regard to its conflict of law provisions, and specifically excluding from application to this Agreement that law known as the United Nations Convention on the International Sale of Goods. You and the Company agree to submit to the personal jurisdiction of the courts located within the county of Santa Clara, California. The failure of the Company to exercise or enforce any right or provision of this Agreement shall not constitute a waiver of such right or provision.

Exhibit D attached hereto.

19. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District and because Defendants are headquartered in this District. It is also proper pursuant to the forum selection clause contained in Defendants' Terms of Service, as set forth above.

FACTUAL BACKGROUND

A. Defendants and Their PII Collection Practices

20. Defendants offer a variety of fee-based services to small businesses, including website hosting (which provides website-building tools), business email (businesses can use their own email name while utilizing the underlying Yahoo Mail architecture), and marketing

and advertising services (collectively "Small Business Services"). To utilize these offerings, users must set up online user accounts, which require them to provide Defendants with PII.

B. Class Members Depend on Defendants Maintaining Reasonable PII Security Practices

21. Defendants understand that online security is paramount to their small business customers and highly material to those customers' decision to utilize Defendants' Small Business Services. Defendants address these concerns on their website for would-be customers considering purchase of the Small Business Services. All small business customers, including Mr. Neff, were exposed to and read Defendants' security claims, because they appear on the webpages all customers must review and use to sign up for Small Business Services.

22. The current (last viewed on January 18, 2017) webhosting services page similarly assures, under the "Secure and reliable" tab, that webhosting is safe and secure, highlighting the following points:

> Secure and reliable
>
> Web Hosting sites are up and running 99.9% of the time.
>
> Your website is backed up in different geographic locations so it will stay live in an emergency.
>
> Your website runs on a Unix operating system and Apache servers.
>
> Password protection is available for your accounts and sections of your website (Advanced and Premier plans only).
>
> Shared SSL certificates and encryption protect the information customers submit to your site (Advanced and Premier plans only).
>
> For an additional fee, you can sign up for the Norton Secured Seal to establish even more credibility with customers. Learn more

Exhibit C attached hereto. Upon information and belief, the webhosting page gave similar assurances throughout the relevant time period.

23. The relationship between Defendants and Class Members is governed by Defendants' Terms of Service ("Terms of Service"), which incorporate by reference a number of other agreements, including Defendants' Privacy Policy ("Privacy Policy"). Throughout the

relevant time, the Terms of Service was a "click-through" agreement. Each member of the Class, including Mr. Neff, prior to becoming a small business customer, was required to click a box stating that "I agree to the terms of service," with the phrase"terms of service" being a live link to the Terms of Service page that would open when clicked. Exhibit D hereto.

24. The Terms of Service expressly refer to both Aabaco and Yahoo, stating as follows:

> This website and the services and products offered are provided by Aabaco Small Business, LLC and its subsidiaries (the "Company") subject to the following Terms of Service ("Terms"), which may be updated from time to time without notice to the user ("You", "Your", or "Merchant"). The Company is a wholly-owned subsidiary of Yahoo! Inc ("Yahoo"). By accessing and using this website and the services and products offered on it, You accept and agree to be bound by the Terms. In addition, when using this website, the services, or products, You will be subject to any posted guidelines or rules applicable to such services, which may be posted and modified from time to time. All such guidelines and rules, including the Privacy Policy, the Site Guidelines, and certain third party agreements as described below, are hereby incorporated by reference into these Terms (all together, the "Agreement").

Exhibit D attached hereto.

25. The Privacy Policy has been updated over the years but, as relevant to this action, always contained identical or substantively similar assurances that Defendants would appropriately safeguard the PII entrusted to them. The Privacy Policy in effect throughout the relevant time represented that:

> CONFIDENTIALITY AND SECURITY
>
> We limit access to Personal Information about You to employees, contractors, or service providers who we believe reasonably need to come into contact with that information to provide products or services to You or in order to do their jobs.
>
> We have physical, electronic, and procedural safeguards that comply with federal regulations to protect Personal Information about You.

Exhibit E attached hereto.

26. In addition, the Privacy Policy represented that Defendants do not share Personal Information except in the following circumstances:

> INFORMATION SHARING AND DISCLOSURE
>
> The Company does not rent, sell, or share Personal Information about You with other people or non-affiliated companies except to provide products or services You've requested, when we have Your permission, or under the following circumstances:
>
> **Service Providers, Contractors, and Agents**: We provide information to partners who work on behalf of or with the Company under confidentiality agreements. These companies do not have any independent right to share this information.
>
> **Co-Branded Partners**: The Company may provide some services in partnership with others under a co-branded experience. In these situations both companies may be collecting information about You so please see the privacy links available within the experience to learn more. For example, Business Mail is provided in partnership with Yahoo.
>
> **Legal Process**: We respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims.
>
> **Security & Fraud**: We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of the Terms of Service, or as otherwise required by law.
>
> **Merger & Acquisition**: We transfer information about You if the Company is acquired by or merged with another company.

27. As Mr. Neff and Class Members would discover in 2016, these material representations about security were false and misleading, because Defendants failed to disclose that their Small Business Services were not secure, given that the PII Mr. Neff and Class Members had entrusted to Defendants was not reasonably safeguarded.

28. In 2012, over 400,000 unencrypted Yahoo usernames and passwords were stolen and posted on a public website.[3] In 2013, Yahoo Japan was compromised, exposing 22 million Yahoo Japan email addresses.[4]

[3] *See, e.g.*, Charles Arthur, *Yahoo Voice Hack Leaks 450,000 Passwords*, The Guardian (July 12, 2012), *available at* https://www.theguardian.com/technology/2012/jul/12/yahoo-voice-hack-attack-

29. Despite experiencing these significant data breaches, Defendants continued to utilize outdated security methods. As reported by Reuters on December 18, 2016, Yahoo utilized an encryption protocol called MD5 that was considered inadequate by online security professionals years before Yahoo finally changed to better encryption in 2013 after the 2013 Data Breach. A public warning was issued about the inadequacy of MD5 in 2008:[5]

> In 2008, five years before Yahoo took action, Carnegie Mellon University's Software Engineering Institute issued a public warning to security professionals through a U.S. government-funded vulnerability alert system: MD5 "should be considered cryptographically broken and unsuitable for further use."
>
> Yahoo's failure to move away from MD5 in a timely fashion was an example of problems in Yahoo's security operations as it grappled with business challenges, according to five former employees and some outside security experts. Stronger hashing technology would have made it more difficult for the hackers to get into customer accounts after breaching Yahoo's network, making the attack far less damaging, they said.
>
> "MD5 was considered dead long before 2013," said David Kennedy, chief executive of cyber firm TrustedSec LLC. "Most companies were using more secure hashing algorithms by then." He did not name specific firms.

Upon information and belief, Yahoo received the MD5 security alert through the government alert system, but it deliberately chose to continue using MD5 for reasons of cost and profitability. As reported by Reuters, former Yahoo security personnel told Reuters that "the security team was at times turned down when it requested new tools and features such as strengthened cryptography protections, on the grounds that the requests would cost too much money, were too complicated, or were simply too low a priority." *See Id.*.

---

passwords-stolen (last visited Feb. 8, 2017); Chenda Ngak, *Yahoo Confirms Email Hack In Statement*, CBS NEWS (July 12, 2012), *available at* http://www.cbsnews.com/news/yahoo-confirms-email-hack-in-statement/ (last visited Feb. 8, 2017).

[4] Graham Cluley, *22 Million User Ids May Be In The Hands Of Hackers, After Yahoo Japan Security Breach*, Naked Security (May 20, 2013), *available at* https://nakedsecurity.sophos.com/2013/05/20/yahoo-japan-hack/ (last visited December 20, 2016); BBC Technology, *Millions Hit By Yahoo Japan Hack Attack*, BBC (May 20, 2013), available at http://www.bbc.com/news/technology-22594136 (last visited December 20, 2016).

[5] *Yahoo security problems a story of too little, too late.* Reuters (December 18, 2016), *available at* http://www.reuters.com/article/us-yahoo-cyber-insight-idUSKBN1470WT (last visited Feb. 8, 2017).

30. In addition, according to a former Yahoo executive quoted in a September 30, 2016 article on Business Insider, Yahoo kept all user data in one database. Notably, this article was published after the 2014 Data Breach was announced and prior to disclosure of the 2013 Data Breach, and the point of the article was to express the executive's skepticism that the 2013 Data Breach impacted "only" 500 million. As the Class learned, the executive was right, Defendants' security breaches impacted more than a billion customers:

> "I believe it to be bigger than what's being reported," the executive, who no longer works for the company but claims to be in frequent contact with employees still there, including those investigating the breach, told Business Insider. "How they came up with 500 is a mystery."
>
> To be sure, Yahoo has said that the breach affected at least 500 million users. But the former Yahoo exec estimated the number of accounts that could have potentially been stolen could be anywhere between 1 billion and 3 billion.
>
> ***
>
> According to this executive, all of Yahoo's products use one main user database, or UDB, to authenticate users. So people who log into products such as Yahoo Mail, Finance, or Sports all enter their usernames and passwords, which then goes to this one central place to ensure they are legitimate, allowing them access.
>
> That database is huge, the executive said. At the time of the hack in 2014, inside were credentials for roughly 700 million to 1 billion active users accessing Yahoo products every month, along with many other inactive accounts that hadn't been deleted.
>
> In late 2013, Yahoo CEO Marissa Mayer said the company had 800 million monthly active users globally. It currently has more than 1 billion.
>
> "That is what got compromised," the executive said. "The core crown jewels of Yahoo customer credentials."[6]

31. Likewise, the technology industry is rife with similar examples of hackers targeting users' PII, including the hacks at Adobe,[7] LinkedIn, eHarmony,[8] and Snapchat,[9]

[6] Paul Szoldra, *A Yahoo insider believes the hackers could really have stolen over 1 billion accounts*, Business Insider (Sept. 30, 2016), *available at*: http://www.businessinsider.com/yahoo-insider-hacking-2016-9 (last visited Feb. 8, 2017).

[7] *See In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014).

[8] CBS News Staff, eHarmony Suffers Password Breach on Heels of Linkedln, CBS News (June 7, 2012), available at http://www.cbsnews.com/news/eharmony-suffers-password-breach-on-heels-of-linkedin/ (last visited December 20, 2016).

among many others, all of which pre-date the time frame Yahoo has identified regarding the Data Breaches. As a company in the online services arena, which employs security professionals, Yahoo undoubtedly knew about these hacks and the high risk that it could suffer similar hacks.

C. Stolen PII Is Valuable to Hackers and Thieves

32. It is well known and has been the subject of many media reports that PII is highly coveted by and a frequent target of hackers. PII is often easily taken because it may be less protected and regulated than payment card data. Especially in the technology industry, the issue of data security and threats thereto is well known, as noted above. Several other online companies have experienced data breaches resulting in the disclosure of users' PII, and as identified earlier, a large number of technology companies have suffered data breaches. Despite well-publicized litigation and frequent public announcements of data breaches by retailers and technology companies, Yahoo opted to maintain an insufficient and inadequate system to protect the PII of Mr. Neff and the Class.

33. Legitimate organizations and the criminal underground alike recognize the value of PII. Otherwise, they wouldn't aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million users, they also took registration data from 38 million users."[10] Similarly, in the Target data breach, in addition to data pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 users.

34. It is well known that the theft of PII can lead directly to identity theft. One form of identity theft, described as "synthetic identity theft," occurs when thieves create new identities by combining real and fake identifying information and then use those identities to open new accounts. "This is where they'll take your Social Security number, my name and

---

[9] Nancy Blair & Brett Molina, *Snapchat, Skype Have Security Breach*, USA Today (Jan. 2, 2014), available at http://www.usatoday.com/story/tech/2014/01/01/snapchat-user-names-leak/4277789/ (last visited December 20, 2016).

[10] Verizon 2014 PCI Compliance Report, available at http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited December 20, 2016).

address, someone else's birthday and they will combine them into the equivalent of a bionic person," said Adam Levin, Chairman of IDT911, which helps businesses recover from identity theft. Synthetic identity theft is harder to unravel than traditional identity theft; experts say: "It's tougher than even the toughest identity theft cases to deal with because they can't necessarily peg it to any one person." In fact, the fraud might not be discovered until an account goes to collections and a collection agency researches the Social Security number. Notably, Mr. Neff experienced exactly this scenario when a credit card was opened in his name in May 2015 without his knowledge and permission.

35. Unfortunately, and as is alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of third parties, such as technology companies, Yahoo's approach to maintaining the privacy of Mr. Neff's and Class Members' PII was lackadaisical, cavalier and reckless, or at the very least, negligent.

D. These Data Breaches Have and Will Result in Additional Identity Theft and Identify Fraud

36. The ramifications of Defendants' failure to keep Mr. Neff's and Class Members' PII secure have been severe.

37. The information Defendants compromised, including Mr. Neff's and Class Members' PII, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC").[11] Identity theft occurs when someone uses another person's identifying information, such as that person's name, address, social security number, credit card number, credit card expiration date, and/or other information, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year.

[11] FTC Interactive Toolkit, *Fighting Back Against Identity Theft*, *available at* http://www.vanderbilt.edu/PersonalIdentityTheftProtection.pdf (last visited Feb. 8, 2017). Io FTC, Signs of Identity Theft, available at https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited December 20, 2016).

38. As alleged above, Mr. Neff experienced three (3) incidents of actual identity theft following the Data Breaches: fraudulent charges appeared on two of his bank cards and an unauthorized credit card account was opened in his name.

39. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[12]

40. According to Javelin Strategy and Research, "almost 1 in 4 consumers that received a data breach letter became a victim of identity fraud."[13] Nearly half (46%) of consumers with a breached debit card became fraud victims within the same year.

41. Identity thieves can use personal information, such as that of Mr. Neff and Class Members, which Defendants failed to secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years. The IRS paid out $43.6 billion in potentially fraudulent returns in 2012, and the IRS identified more than 29 million incidents of identity theft in 2013. The IRS described identity theft as the number one tax scam for 2014.

42. Among other forms of fraud, identity thieves may get medical services using customers' compromised personal information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

43. It is incorrect to assume that reimbursing a customer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving

[12] *See 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, *available at* https://www.javelinstrategy.com/coverage-area/2013-identity-fraud-report-data-breaches-becoming-treasure-trove-fraudsters (last visited Feb. 8, 2017) (the "2013 Identity Fraud Report").

[13] *Id.*

problems."[14] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id.* at 11.

E. Annual monetary losses from identity theft are in the billions of dollars.

44. Javelin Strategy and Research reports that those losses increased to $21 billion in 2013.[15]

45. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

46. Mr. Neff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, regardless of whether such charges are ultimately reimbursed by the credit card companies.

F. Plaintiff and Class Members Suffered Damages As A Result of the Data Breach

47. The Data Breaches were a direct and proximate result of Defendants' failure to properly safeguard and protect Mr. Neff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of

---

[14] Victims of Identity Theft, 2012 (Dec. 2013) at 10, *available at* https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited December 20, 2016).

[15] *See* 2013 Identity Fraud Report.

[16] GAO, Report to Congressional Requesters at 33 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (emphases added) (last visited Feb. 8, 2017).

Mr. Neff's and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information. As alleged above, Defendants used outdated encryption protocol DB5 years after industry warnings about its obsolescence and utilized one giant database for the storage of PII for all of their customers, presenting hackers with an irresistible target and ensuring that any breach would be much broader in scope than if the information had been less concentrated. Moreover, as alleged above, Yahoo security employees have stated to reporters that Yahoo failed to heed warnings from them because of cost concerns.

48. Mr. Neff's and Class Members' PII is private and sensitive in nature and was left inadequately protected by Defendants. Defendants did not obtain Mr. Neff's and Class Members' consent to disclose their PII, except to certain persons not relevant to this action, as required by applicable law and industry standards.

49. As a direct and proximate result of Defendants' wrongful action and inaction and the resulting Data Breaches, Mr. Neff (as addressed above) and Class Members have been damaged by paying monthly fees to Defendants in exchange for the Small Business Services, given that safeguarding customer data was an express provision of the terms of the contract between Defendants and Class Members, as alleged above, which provision Defendants breached, as also alleged above. Accordingly, Mr. Neff and the Class Members have suffered out-of-pocket damages equal to the monthly fees they paid or, at least, a portion of such fees.

50. In addition, as a direct and proximate result of Defendants' wrongful action and inaction and the resulting Data Breaches, Mr. Neff (as was addressed above) and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Data Breaches on their lives by, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

51. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Mr. Neff's and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals and already misused via the sale of their information on the Internet black market;

c. the untimely and inadequate notification of the Data Breaches;

d. the improper disclosure of their PII;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breaches;

g. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

h. overpayments to Defendants for the Small Business Services in that a portion of the price paid for them by Plaintiffs and Class Members was for the costs of reasonable and adequate safeguards and security measures that would protect users' PII, which Defendants did not implement and, as a result, Plaintiff and Class Members did not receive what they paid for and were overcharged by Defendants; and

i. deprivation of rights they possess under the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200).

52. While the PII of Plaintiff and the members of the Class was stolen, the same or a copy of the same or updated PII continues to be held by Defendants. Plaintiff and the members

of the Class have an undeniable interest in insuring that this information is secure, remains secure, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

53. Mr. Neff seeks relief in his individual capacity and as representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2), (b)(3), and (c)(4), Plaintiff seeks certification of a nationwide class initially defined as follows:

> All Yahoo Small Business and Aabaco Small Business customers residing in the United States whose Personal Identifying Information was disclosed in the 2013 Data Breach or the 2014 Data Breach (the "Class").

54. Excluded from the Class are Defendants, including any entity as to which either Defendant holds a controlling interest, is a parent or subsidiary, or which is controlled by either Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants. Also excluded are all judges and court personnel who ever handle this case and all members of their immediate families.

55. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Mr. Neff at this time, Defendants have acknowledged that the PII of more than 1 billion users was affected by the Data Breaches, including Mr. Neff's.

56. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants violated the California's Unfair Competition Law by failing to implement reasonable security procedures and practices;

b. Whether Defendants violated common and statutory law by failing to promptly notify Class Members that their PII had been compromised;

c. Whether Class Members may obtain injunctive relief against Defendants under California's privacy laws to require that it safeguard or destroy, rather than retain, the PII of Class Members;

d. Which security procedures and which data-breach notification procedure Defendants should be required to implement as part of any injunctive relief ordered by the Court;

e. Whether Defendants had an express or implied contractual obligation to use reasonable security measures;

f. Whether Defendants breached their express or implied contractual obligation to use reasonable security measures;

g. What security measures, if any, must be implemented by Defendants to comply with their express or implied contractual obligations;

h. Whether Defendants violated California's privacy laws in connection with the actions described here; and

i. What relief, including equitable relief, should be awarded to the Class Members.

57. All members of the proposed Class are readily ascertainable. Defendants know which customer accounts were compromised by the Data Breaches, and they have access to email addresses, physical addresses, and other contact information for the millions of members of the Class, which information can be used to provide notice to them.

58. Typicality. Fed. R. Civ. P. 23(a)(3). Mr. Neff's claims are typical of those of the other Class Members, because his PII, like that of every other Class Member, was misused and/or disclosed by Defendants in the same manner.

59. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Mr. Neff will fairly and adequately represent and protect the interests of the other members of the Class, because he has no conflicts of interest with them. Further, Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation.

60. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable and the court system could not handle individual suits by even a fraction of them. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. Finally, there will be no difficulty in the management of this action as a nationwide class action, in part because the Terms of Service make California law applicable to all Class Members.

61. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Yahoo's violations of law inflicting substantial damages in the aggregate would go un-remedied. A class action is superior to no potential method for Class Members to recover their losses.

62. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Defendants have acted or have refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

COUNT I

Breach of Contract
(On Behalf of Plaintiff and the Class)

63. Plaintiff incorporates the substantive allegations contained in Paragraphs 1 through 62.

64. The Terms of Service and its incorporated Privacy Policy formed written contracts between Defendants and Plaintiff and the Class.

65. Plaintiff and the Class performed their end of the bargain, complying with all provisions applicable to them.

66. As written in the Privacy Policy, and as alleged above, Defendants made the following express terms of the contracts: "We limit access to Personal Information about You to employees, contractors, or service providers who we believe reasonably need to come into contact with that information to provide products or services to You or in order to do their jobs.

We have physical, electronic, and procedural safeguards that comply with Federal regulations to protect Personal Information about You." Exhibit E attached hereto.

67. In addition, the written contracts between Defendants and Plaintiff and the Class included an implied duty on Defendants' part to reasonably protect Plaintiff's and Class Members' PII.

68. Defendants breached these express and implied terms of the written contracts by failing to limit access to Plaintiff's and Class Members' PII as promised and by failing to reasonably protect their PII, including by using an inadequate encryption protocol.

69. As a direct and proximate result of Defendants' breaches of their written contracts with Plaintiff and Class Members, Plaintiff and Class Members sustained actual losses and damages as described in detail above.

COUNT II

Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

70. Plaintiff incorporates the substantive allegations contained in Paragraphs 1 through 62.

71. Defendants solicited and invited Plaintiff and the members of the Class to use their services. Plaintiff and Class Members accepted Defendants' offers and created user accounts requiring the provision of PII with Defendants prior to the Data Breaches.

72. When Plaintiff and Class Members used Defendants' services and products, they provided their PII. In so doing, Plaintiff and Class Members entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if their PII had been breached and compromised.

73. Each use of Defendants' Small Business Services by Plaintiff and Class Members was made pursuant to their mutually agreed-upon implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect Plaintiff's and Class Members' PII and to timely and accurately notify them if such information was compromised or stolen.

74. Plaintiff and Class Members would not have provided and entrusted their PII to Defendants in the absence of the implied contracts between them and Defendants.

75. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendants.

76. Defendants breached the implied contracts they made with Plaintiff and Class Members by failing to safeguard and protect the PII of Plaintiff and Class Members and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breaches.

77. As a direct and proximate result of Defendants' breaches of their implied contracts with Plaintiff and Class Members, Plaintiff and Class Members sustained actual losses and damages as described in detail above.

COUNT III

Negligence
(On Behalf of Plaintiff and the Class)

78. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 62.

79. Upon accepting and storing Plaintiff's and Class Members' PII in their respective computer database systems, Defendants undertook and owed a duty to Plaintiff and Class Members pursuant to the common law and Cal Civ. Code § 1748.815 to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so. Defendants knew, acknowledged, and agreed that the PII was private and confidential and would be protected as private and confidential.

80. Defendants breached their duty to Plaintiff and the Class Members to adequately protect and safeguard their PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering their negligent practices, Defendants failed to provide adequate supervision and oversight of the PII with which they were entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to steal

Plaintiff's and Class Members' PII, misuse the PII, and intentionally disclose it to others without consent.

81. Under both common law and statutory law (including, as alleged below, pursuant to California's PII protection statute, Cal. Civ. Code § 1798.81.5), Defendants had an affirmative duty to timely discover and disclose the unauthorized access and theft of the PII to Plaintiff and the Class so that Plaintiff and Class Members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

82. Defendants breached their duty to timely discover and notify Plaintiff and Class Members of the Data Breaches by allegedly failing to discover and by failing to notify Plaintiff and Class Members of the 2013 and 2014 Data Breaches until September and December 2016. To date, Defendants have not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access for Plaintiff and Class Members to adequately protect themselves, such that Defendants continue to breach their disclosure obligations to Plaintiff and the Class. Specifically, the information provided to the Class in the email notice discussed above, and attached as Exhibit A hereto, is lacking detail. The Class still does not know exactly what information was taken, who took it, whether and how it has been disseminated and used, and what can be done to protect themselves.

83. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and their failure to protect Plaintiff's and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Defendants breached their duty to use reasonable care to adequately protect and secure Plaintiffs and Class Members' PII during the time it was within Defendants' possession or control. At the very least, Defendants should have abandoned the MD5 encryption protocol for more secure ones, as the online security world was told to do years before Defendants complied with the recommendations, and, moreover, Defendants should not have kept the PII of the entire Class in one giant database.

84. Further, through their failure to timely discover and provide a timely and clear notification of the Data Breaches to customers, as required by Cal. Civ. Code § 1798.82,

Defendants prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII, including other online accounts.

85. Upon information and belief, Defendants improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation from standard industry rules, regulations, and practices at the times of the Data Breaches.

86. Defendants' failure to take proper security measures to protect Plaintiffs and Class Members' sensitive PII, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized theft of Plaintiff's and Class Members' PII.

87. Defendants' conduct was negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII as evidenced by Defendants' use of the outdated MD5 encryption protocol, and utilization of a single database that contained PII of all users; failing to conduct adequate regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class Members' PII.

88. Neither Plaintiff nor the other Class Members contributed to the Data Breaches and subsequent misuse of their PII as described in this Complaint. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members sustained actual losses and damages as described in detail above.

COUNT IV

Fraudulent Inducement

(On Behalf of Plaintiff and the Class)

89. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 62.

90. Defendants made numerous representations on their website, on the webpages describing the Small Business Services, and in the Privacy Agreement incorporated into the Terms of Service, regarding the supposed secure nature of their Small Business Services. Such representations were false, because, among other reasons, Defendants utilized outdated

encryption protocols. Defendants also failed to disclose that they did not use reasonable, industry-standard means to safeguard against hacking and theft of customer PII. Such omissions were material, because no reasonable person would pay for services such as webhosting and business email that would unreasonably expose their PII to theft and expose them to identity theft.

91. Because the misrepresentations and omissions were material to customers and would-be customers, including Plaintiff and the Class, they reasonably relied on them. Plaintiff and other members of the Class would not have agreed to utilize and pay for the Small Business Services and turn over their PII to Defendants had they known the truth: that Defendants' services were not as secure as represented or secure at all.

92. Defendants intended for Plaintiff and other Class members to rely on their security misrepresentations and omissions, as they knew no would-be customer would submit PII to them or entrust an online business to unreasonable security risks, much less pay for such risk.

93. Defendants had experienced several data breaches prior to the 2013 breach (and after), had been warned that their encryption was outdated, and rejected the advice from their own security employees or contractors to improve security. Defendants' representations and omissions were made with knowledge of their falsity or, at least, with extreme disregard for their truth.

94. As a direct and proximate result of Defendants' wrongful action and inaction, Plaintiff and the other Class members have been damaged by paying monthly fees to Defendants for something they did not receive: secure Small Business Services. Plaintiff and the other Class members were also damaged by experiencing actual identity theft (as in Plaintiff's case) and/or placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Data Breaches on their lives.

COUNT V

Negligent Misrepresentation
(In The Alternative To The Claim For Fraudulent Inducement)
(On Behalf of Plaintiff and the Class)

95. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 62.

96. Defendants made numerous representations on their website, on the webpages describing the Small Business Services and in the Privacy Agreement incorporated into the Terms of Service, regarding the supposed secure nature of their Small Business Services. Such representations were false, among other reasons, because Defendants utilized outdated encryption protocols. Defendants also failed to disclose that they did not use reasonable, industry-standard means to safeguard against hacking and theft of customer PII. Such omissions were material, because no reasonable person would pay for services such as webhosting and business email that would unreasonably expose their PII to theft and expose them to identity theft.

97. Because the misrepresentations and omissions were material to customers and would-be customers, including Plaintiff and the Class, they reasonably relied on them. Plaintiff and other members of the Class would not have agreed to utilize and pay for the Small Business Services and turn over their PII to Defendants had they known the truth: that Defendants' services were not as secure as represented or secure at all.

98. Defendants intended for Plaintiff and other Class members to rely on their security misrepresentations and omissions, as they knew no would-be customer would submit PII to them or entrust an online business to unreasonable security risks, much less pay for such risk.

99. Defendants had experienced several data breaches prior to the 2013 breach (and after), had been warned that their encryption was outdated, and rejected the advice from their own security employees or contractors to improve security. Defendants' representations and omissions were made without any reasonable ground for believing that they were true.

100. As a direct and proximate result of Defendants' wrongful action and inaction, Plaintiff and the other Class members have been damaged by paying monthly fees to Defendants for something they did not receive: secure Small Business Services. Plaintiff and the other Class members were also damaged by experiencing actual identity theft (as in Plaintiff's case) and/or placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Data Breaches on their lives.

COUNT VI

Violation of California's Unfair Competition Law Cal. Bus. & Prof. Code § 17200 — Unlawful Business Practices
(On Behalf of Plaintiff and the Class)

101. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 62.

102. Defendants have violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200. Defendants engaged in unlawful acts and practices with respect to their services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class Members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which required Defendants to use reasonable methods of safeguarding the PII of Plaintiff and the Class Members.

103. In addition, Defendants engaged in unlawful acts and practices with respect to their services by failing to discover and then disclose the Data Breaches to Plaintiff and Class Members in a timely and accurate manner so that they could take action to protect themselves from identity theft, contrary to the duties imposed by Cal. Civ. Code § 1798.82. To date, Defendants have still not provided sufficient information to Plaintiff and the Class Members.

104. As a direct and proximate result of Defendants' unlawful acts and practices, Plaintiff and the Class Members were injured and lost money or property, including, but not limited to, the loss of their legally protected interest in the confidentiality and privacy of their PII, plus additional losses described above.

105. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data breach or theft was high. Defendants' actions in engaging in the above-described unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Class Members.

106. The members of the Class seek relief under Cal. Bus. & Prof. Code § 17200, *et. seq.*, including, but not limited to, restitution to Plaintiff and Class Members of money or property that Defendants acquired by means of their unlawful and unfair business practices (including the monthly fees Defendants collected from Plaintiff and the Class), restitutionary disgorgement of all profits accruing to Defendants because of their unlawful and unfair business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT VII

Violation of California's Unfair Competition Law Cal. Bus. & Prof. Code § 17200 — Unfair Business Practices
(On Behalf of Plaintiff and the Class)

107. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 62.

108. Defendants engaged in unfair acts and practices by soliciting and collecting Plaintiff's and Class Members' PII with knowledge that the information would not be adequately protected and by storing Plaintiff's and the Class Members' PII in an unsecure electronic environment, all without disclosing same. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Class Members. They were likely to deceive the public into believing their PII

was securely stored, when it was not. The harm these practices caused to Plaintiffs and the members of the Class outweighed their utility, if any.

109. Defendants engaged in unfair acts and practices with respect to the provision of their services by failing to utilize adequate privacy and security measures and protect Class Members' PII from unauthorized disclosure, release, data breaches, and theft, and by failing to timely discover and give notice of the Data Breaches. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class Members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiff and Class Members outweighed their utility, if any.

110. As a direct and proximate result of Defendants' unfair practices and acts, Plaintiff and the members of the Class were injured and lost money or property, including, but not limited to, the loss of their legally protected interest in the confidentiality and privacy of their PII, plus additional losses described above.

111. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data breach or theft was high. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Class members.

112. The members of the Class seek relief under Cal. Bus. & Prof. Code § 17200, *et. seq.*, including, but not limited to, restitution to Plaintiff and Class Members of money or property that the Defendants acquired by means of their unfair business practices (including the monthly fees they collected from Plaintiff and the Class), restitutionary disgorgement of all profits accruing to Defendants because of their unfair business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT VIII

Violation of California's Unfair Competition Law Cal. Bus. & Prof. Code § 17200 — Fraudulent/Deceptive Business Practices
(On Behalf of Plaintiff and the Class)

113. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 62.

114. Defendants engaged in fraudulent and deceptive acts and practices by representing on its website, that: (a) it would maintain adequate data privacy and security practices and procedures to safeguard the Class Members' PII from unauthorized disclosure, release, data breaches, and theft; and (b) it did and would comply with the requirements of relevant law pertaining to the privacy and security of the Class Members' PII. These representations were likely to deceive members of the public, including Plaintiff and the members of the Class, into believing their PII was securely stored, when it was not, and that Defendants were complying with relevant law, when they were not.

115. Defendants engaged in fraudulent and deceptive acts and practices by omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Class Members' PII. At the time that Class Members were using Defendants' services, Defendants failed to disclose to Class Members that their data security systems failed to meet legal and industry standards for the protection of their PII. Plaintiffs would not have purchased Defendants' Small Business Services if they had known about Defendants' substandard data security practices. These omissions were likely to deceive members of the public, including Plaintiff and the Class Members, into believing their PII was securely stored, when it was not, and that Defendants were complying with relevant law and industry standards, when they were not.

116. As a direct and proximate result of Defendants' deceptive practices and acts, Plaintiff and the Class Members were injured and lost money or property, including, but not limited to, the loss of their legally protected interest in the confidentiality and privacy of their PII, plus additional losses described above.

117. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data breach or theft was high. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Class members.

118. Class Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and Class Members of money or property that Defendants acquired by means of their fraudulent and deceptive business practices (including the monthly fees they collected from Plaintiff and the Class members), restitutionary disgorgement of all profits accruing to Defendants because of their fraudulent and deceptive business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, Brian Neff, individually and on behalf of all Class Members proposed in this Complaint, respectfully requests the Court to enter judgment in his favor and against Defendants as follows:

a. For an Order certifying the Class and appointing Plaintiff and his Counsel to represent the Class;

b. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of here pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiff and Class Members;

c. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to customer data collection, storage, and safety and to disclose with specificity to Class Members the type of PII compromised;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e. For an award of actual damages and compensatory damages, in an amount to be determined;

f. For an award of costs of suit and attorneys' fees, as allowable by law;

g. For an award of pre-judgment and post-judgment interest at the maximum rates permitted at law or in equity; and

h. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

Dated: February 8, 2017

MILBERG LLP
DAVID AZAR

/s/ David Azar
DAVID AZAR
2850 Ocean Park Blvd. Suite 300
Santa Monica, CA 90405
Telephone: (213) 617-1200
Facsimile: (212) 868-1229
E-mail: dazar@milberg.com

MILBERG LLP
Ariana J. Tadler
Henry J. Kelston
Andrei V. Rado
One Pennsylvania Plaza
New York, New York 10119
(212) 594-5300

LACKEY HERSHMAN, L.L.P.
Roger L. Mandel
rlm@lhlaw.net
Bruce E. Bagelman
beb@lhlaw.net
3102 Oak Lawn Avenue, Suite 777
Dallas, Texas 75219-4259
Telephone: (214) 560-2201
Telecopier: (214) 560-2203

Attorneys for Plaintiff and the Proposed Class